INPUT®

IT Intelligence Services

Saida Building, 4-6, Kanda Sakuma-cho
Chiyoda-ku, Tokyo 101
Tel. +81 (03) 3864-0531
Fax +81 (03) 3864-4114

FAX TRANSMITTAL FORM

Date : Feb. 10, 1995

To : Name : Tom O'Flaherty

Tel/Location : 201-801-0050

Co : INPUT NJ

Fax No. : 201-801-0441

From : Yoshiko Wakaki/INPUT KK

Subject : Internet Security Study for NTT Data

Confidential : Y / N
Urgent : Y / N

Page : 1 of 1

File : CHRON
CONTACT
OTHER :

NTT Data wishes to receive the report by the end of March. Please make arrangements for beginning ~~the~~ work to meet this requirement. We will receive their authorization on Monday, 2/13.

Tetsuro

4339

INPUT®

IT Intelligence Services

400 Frank W. Burr Blvd.
Teaneck, NJ 07666
Tel. (201) 801-0050
Fax (201) 801-0441

FAX TRANSMITTAL FORM

Date: 2/10/95

Confidential: Y / N
Urgent: Y / N

To: Name: Renée

Tel./Location:

Co.:

Page: 1 of 8

Fax No: Ynette ↓

File: Chron
Contact
Other:

From: Name:

Subject: Cy Tog.. NTT (Japan)

(YNNT3)

Hi its me again.
Smile its Friday!

O.K I'll Fax this Again
its only my third time.

Keep Smiling!

Proposal

INTERNET SECURITY: SECURE HTTP AND SECURE SOCKET LAYER

Submitted to

NTT Data Communications Systems

January 17, 1995

Submitted by

INPUT

Atrium at Glenpointe
400 Frank W. Burr Blvd.
Teaneck, NJ 07666

201-801-0050
201-801-0441

INTERNET SECURITY: SECURE HTTP AND SECURE SOCKET LAYER

I. OBJECTIVES

NTT Data Communications Systems requires information on security for payments executed on the Internet. The focus is on Secure HTTP and Secure Socket Layer, plus other comparable methods.

II. SCOPE

The scope of the study covers the following questions:

- Which vendors are using Secure HTTP, Secure Socket Layer or another method? Which methods are dominant now? In the future?
- What are the marketing plans for these vendors?
- Who are examples of users of these methods?
- Do the vendors have Japanese agents? Are there any barriers to export to Japan?
- What kind of partnership or affiliation arrangements are possible?
- What is the name of a contact person at each vendor?
- Which products use the public key encryption method of RSA? Who provides the public key encryption server?
- Can RSA-equipped products be exported to Japan? What agreements would be necessary for NTT Data to develop a public key encryption service for Japan?
- What kind of partnership or affiliation arrangements are possible with RSA? Does RSA have a Japanese agent? Who is the contact person at RSA?

The study will cover Secure HTTP and Secure Socket Layer and up to two other methods. The detail for the other two methods may be less complete than for Secure HTTP and Secure Socket Layer, since the other methods may be less complete or cover niche areas.

III. METHODOLOGY

INPUT will obtain information from the suppliers involved and other reliable sources. NTT will not be identified as the client for this study. INPUT will collect and forward to NTT Data product descriptions and brochures, company information and other pertinent information.

INPUT can begin work within two weeks of authorization. A written report covering the "Scope" issues will be completed within three weeks after work begins.

IV. FEES

The fee for this study is $13,000. This covers all INPUT expenses. One half of this amount ($6,500) is due and payable upon authorization. the remainder is due upon submission of the report.

V. AUTHORIZATION

To authorize the project as specified, please sign and return one copy of this proposal, along with the initial fee. Upon acceptance by INPUT, a countersigned copy of the proposal will be returned to NTT Data Communications Systems.

AUTHORIZED BY: NTT Data Communication Systems	ACCEPTED BY: INPUT
Name	Name
Title	Title
Date	Date

```
                    ****************************
                    ***   ACTIVITY REPORT    ***
                    ****************************

        TRANSMISSION OK

        TX/RX NO.                 4514
        CONNECTION TEL              011 81 33 864 4114
        CONNECTION ID             JAPAN
        START TIME                01/16 17:11
        USAGE TIME                00'46
        PAGES                       1
        RESULT                    OK
```

```
***************************
***   ACTIVITY REPORT   ***
***************************
```

TRANSMISSION OK

TX/RX NO.	4939
CONNECTION TEL	1 415 961 3967
CONNECTION ID	PROD
START TIME	02/10 11:48
USAGE TIME	05'06
PAGES	8
RESULT	OK

ORDER/INVOICE/FULFILLMENT

Acctg. ONLY

Inv. Comp.	By:	Date:	Client #	Order #	Inv. #	Multi-Invoicing ____ of ____

CUSTOMER/INVOICE TO

ORIGINATOR (Signature) ______ DATE 2/14/95

Company NTT (Japan)
~~Name Mr./Ms.~~ Data Communications Sys
Position ______
Address ______
______
City ______
Province ______
Phone ______

CA Tax Rate ______
CT Tax 8% ______
Salutation ______
State ______
Zip ______
Country ______
Fax ______
Tlx ______

APPROVALS
RR
VP Sales/Res.
2/10
Date
______
Controller
______
Date

Special instructions for invoicing, progress billing, or delayed payments, etc.
Per Japanese process

ORDER

Contract Year Beg. ______
End ______

□ New Order (N1) □ Prior Yr (N3)
□ Renewal (N2) □ Cancel

Invoice Type
□ Fulfillment Only
□ W/Order (OR)
□ Monthly (MO)
□ Quarterly (QT)
□ Pending

Employee # Sold by:
RR 100%
____ %
____ %

~~Employee #~~ Commission to:
KK ____ %
($2,600) ____ %
____ %

CLIENT AUTH.

PO# ______
Attach all authorizing documents to white (contract) copy.

INPUT Contract □ Letter □ Verbal □
See attached fax

SHIP TO

Company ______
Name Mr./Ms. ______
Position ______
Address ______
______
City ______

Province ______
Salutation ______
State ______
Zip ______
Country ______
Phone ______

ITEM TYPE

• Subscription	(SB)	• Copies	(CP)	• Merger/Acq.	(ME)
• Custom	(YC/ZC/KC)VC	• Consult/Present	(PR)	• Exec Overview	(EO)
• Multiclient	(MC)	• Newsletter	(NL)	• Conf/Seminar	(CN)
• Reports	(RP)	• Reimbursed Costs	(EX)		

DETAIL

Indicate US, UK, FR, VA	Prod. ID/Year	Item Type Code	Item Description or Title	Quantity	Price	Shipped By	Date
US	YNNT3		Internet Security		~~$10,000~~		
				(Gross)	$13,000		
			(Expenses				
			inboarded)				

Fulfillment to be completed in: □ Corporate □ London □ Virginia □ France □ Other ______

• White - Contract • Green - Fulfillment • Yellow - Invoice • Pink - Originator • Goldenrod - Sales Manager

Project Work Statement

Prepared by (print): TQ²

Date: 2/10/95

Project Title: Internet Security

Project Code: YNNT3

Client Name*: NTT (Japan)

Project Manager: TQ²

Project Source: □ Program □ Multi-Client □ Custom □ Other

Project Type: □ Report □ Presentation □ Other

Initiation Date: 2/13/95

Begin Production:

Midpoint Review:

Shipping Date:

First Draft Due: 3/31

Resources Required: 6.5 ESD

Level of Effort (number of days): Consultant R/A

Source—Internal/[✓ External] (specify): R. Peterson ≈ 5 days

KK Commission – $2,600

Contract Value: [✓ $] £ ¥ 13,000 gross

Reimbursable Expenses: ☒ No □ Yes

Expense Budget: $ £ ¥ ____________

To Cover: Travel: ____________ Telephone: ____________

Report Preparation: ____________ Other: ____________

Project Description: Assess Internet security products

* Attach list for Multi-Clients **For Custom and Multi-Client Projects

ACCOUNTING USE ONLY: Entered on current project list □

PROJECT SCHEDULE

Activity	Name	Act. Days	Factor	ESD	Week													
					1	2	3	4	5	6	7	8	9	10	11	12	13	14
Research				6½	½	1	2	1	2									
TOTAL PLAN SR.	▨		▨	▨														
TOTAL PLAN RA	▨		▨	▨														
TOTAL PLAN ESDs	▨	▨	▨															

Proj. Code: ______________ Proj. Name: YNNT3 ______________ Prepared by: TR

Page 1 of

Proj. Manager: ______________ Date: 2/10

4938

ORDER/INVOICE/FULFILLMENT

Acctg. ONLY

Inv. Comp.	By:	Date:	Client #	Order #	Inv. #	Multi-Invoicing ___ of ___

CUSTOMER/INVOICE TO

ORIGINATOR (Signature) ________ DATE 2/1/95

Company NTT (Japan)

~~Name Mr./Ms.~~ Data Communications Sys

Position ________

Address ________

____

City ________

Province ________

Phone ________

CA Tax Rate ________

CT Tax 8% ________

Salutation ________

State ________

Zip ________

Country ________

Fax ________

Tlx ________

APPROVALS

VP Sales/Res.

2/10

Date

Controller

Date

Special instructions for invoicing, progress billing, or delayed payments, etc.

Per Japanese process

ORDER

Contract Year Beg. ________

End ________

□ New Order (N1) □ Prior Yr (N3)

□ Renewal (N2) □ Cancel

Invoice Type □ Fulfillment Only

□ W/Order (OR)

□ Monthly (MO)

□ Quarterly (QT)

□ Pending

Employee #
Sold by:
RR 100%
___ ___%
___ ___%

~~Employee #~~
Commission to:
KK ___%
($2,600) ___%
___ ___%

CLIENT AUTH.

PO# ________

Attach all authorizing documents to white (contract) copy.

INPUT Contract □ Letter □ Verbal □

See attached fax

SHIP TO

Company ________

Name Mr./Ms. ________

Position ________

Address ________

____

City ________

Province ________

Salutation ________

State ________

Zip ________

Country ________

Phone ________

ITEM TYPE

- Subscription (SB)
- Custom (YC/ZC/KC)VC
- Multiclient (MC)
- Reports (RP)
- Copies (CP)
- Consult/Present (PR)
- Newsletter (NL)
- Reimbursed Costs (EX)
- Merger/Acq. (ME)
- Exec Overview (EO)
- Conf/Seminar (CN)

DETAIL

Indicate US, UK, FR, VA	Prod. ID/Year	Item Type Code	Item Description or Title	Quantity	Price	Shipped By	Date
US	YNNT3		Internet Security		~~10,000~~		
				(Gross)	$13,000		
			(Expenses				
			inboarded)				

Fulfillment to be completed in: □ Corporate □ London □ Virginia □ France □ Other ________

• White - Contract • Green - Fulfillment • Yellow - Invoice • Pink - Originator • Goldenrod - Sales Manager

Proposal

INTERNET SECURITY: SECURE HTTP AND SECURE SOCKET LAYER

Submitted to

NTT Data Communications Systems

January 17, 1995

Submitted by

INPUT

Atrium at Glenpointe
400 Frank W. Burr Blvd.
Teaneck, NJ 07666

201-801-0050
201-801-0441

INTERNET SECURITY: SECURE HTTP AND SECURE SOCKET LAYER

I. OBJECTIVES

NTT Data Communications Systems requires information on security for payments executed on the Internet. The focus is on Secure HTTP and Secure Socket Layer, plus other comparable methods.

II. SCOPE

The scope of the study covers the following questions:

- Which vendors are using Secure HTTP, Secure Socket Layer or another method? Which methods are dominant now? In the future?
- What are the marketing plans for these vendors?
- Who are examples of users of these methods?
- Do the vendors have Japanese agents? Are there any barriers to export to Japan?
- What kind of partnership or affiliation arrangements are possible?
- What is the name of a contact person at each vendor?
- Which products use the public key encryption method of RSA? Who provides the public key encryption server?
- Can RSA-equipped products be exported to Japan? What agreements would be necessary for NTT Data to develop a public key encryption service for Japan?
- What kind of partnership or affiliation arrangements are possible with RSA? Does RSA have a Japanese agent? Who is the contact person at RSA?

The study will cover Secure HTTP and Secure Socket Layer and up to two other methods. The detail for the other two methods may be less complete than for Secure HTTP and Secure Socket Layer, since the other methods may be less complete or cover niche areas.

III. METHODOLOGY

INPUT will obtain information from the suppliers involved and other reliable sources. NTT will not be identified as the client for this study. INPUT will collect and forward to NTT Data product descriptions and brochures, company information and other pertinent information.

INPUT can begin work within two weeks of authorization. A written report covering the "Scope" issues will be completed within three weeks after work begins.

IV. FEES

The fee for this study is $13,000. This covers all INPUT expenses. One half of this amount ($6,500) is due and payable upon authorization. the remainder is due upon submission of the report.

V. AUTHORIZATION

To authorize the project as specified, please sign and return one copy of this proposal, along with the initial fee. Upon acceptance by INPUT, a countersigned copy of the proposal will be returned to NTT Data Communications Systems.

AUTHORIZED BY: NTT Data Communication Systems	ACCEPTED BY: INPUT
Name ______________________	Name ______________________
Title ______________________	Title ______________________
Date ______________________	Date ______________________

PROJECT SCHEDULE

Activity	Name	Act. Days	Factor	ESD	Week													
					1	2	3	4	5	6	7	8	9	10	11	12	13	14
Research				6½	½	1	2	1	2									
TOTAL PLAN SR.	▨		▨	▨														
TOTAL PLAN RA	▨		▨	▨														
TOTAL PLAN ESDs	▨	▨	▨															

Proj. Code: ______________ Proj. Name: YNNT3 Prepared by: TR

Page 1 of

Proj. Manager: ______________ Date: 2/10

Project Work Statement

Prepared by (print): TQ^2

Date: 2/10/95

Project Title: Internet Security

Project Code: YNNT3

Client Name*: NTT (Japan)

Project Manager: TQ^2

Project Source: □ Program □ Multi-Client □ Custom □ Other

Project Type: □ Report □ Presentation □ Other

Initiation Date: 2/13/95

Begin Production:

Midpoint Review:

Shipping Date:

First Draft Due: 3/31

Resources Required: 6.5 ESD

Level of Effort (number of days): Consultant R/A

Source—Internal/[✓ External] (specify): R. Peterson ≈ 5 days

KK Commission – $2,600

Contract Value: [✓ $] £ ¥ 13,000 gross

Reimbursable Expenses: ☒ No □ Yes

Expense Budget: $ £ ¥ __________

To Cover: Travel: __________ Telephone: __________

Report Preparation: __________ Other: __________

Project Description: Assess Internet security products

* Attach list for Multi-Clients **For Custom and Multi-Client Projects

ACCOUNTING USE ONLY: Entered on current project list □

INPUT®

IT Intelligence Services

Saida Building, 4-6, Kanda Sakuma-cho
Chiyoda-ku, Tokyo 101
Tel. +81 (03) 3864-0531
Fax +81 (03) 3864-4114

FAX TRANSMITTAL FORM

Date : Feb. 10, 1995

Confidential : Y / N
Urgent : Y / N

To : Name : Tom O'Flaherty

Tel/Location : 201-801-0050

Co : INPUT NJ

Fax No. : 201-801-0441

Page : 1 of 1

From : Yoshiko Wakaki/INPUT KK

File : CHRON
CONTACT
OTHER :

Subject : Internet Security Study for NTT Data

NTT Data wishes to receive the report by the end of March. Please make arrangements for beginning ~~the~~ work to meet this requirement. We will receive their authorization on Monday, 2/13.

Tetsu

```
****************************
***   ACTIVITY REPORT    ***
****************************
```

TRANSMISSION OK

TX/RX NO.	4514
CONNECTION TEL	011 81 33 864 4114
CONNECTION ID	JAPAN
START TIME	01/16 17:11
USAGE TIME	00'46
PAGES	1
RESULT	OK

Report

SECURITY FOR INTERNET TRANSACTIONS

Submitted to

NTT DATA COMMUNICATION

March 17, 1995

Submitted by

INPUT

Atrium at Glenpointe
400 Frank W. Burr Boulevard
Teaneck, NJ 07666

201-801-0050
Fax: 201-801-0441

Four Methods for Securing Payments Executed on the Internet

I. RSA Data Security

A. Background -- RSA is the leading supplier of public and private key encryption algorithms. Their block cypher algorithm technology uses variants of the digital encryption standard (DES). (See Attachment 1 for a complete package of literature)

1. Recent products include:
   a. RC5 Symmetric Block Cypher -- an alternative to DES
   b. RSA Secure --a harddisk encryption software product
   c. RSA Tipem 1.5 -- an upgrade for their software toolkit for securing electronic messages
2. Developer's Toolkits include:
   a. Mail Safe -- an older, DOS-based product for encryption and authentication
   b. Certificate Issuing System (CIS) -- latest technology from RSA for issues digital certificates where the identity is bound to the key.

B. Market -- RSA technology is available in a number of ways (examples of vendors offering this option are noted):

1. Turnkey application - EIT and their CommerceNet offering
2. Product applications
   a. Netscape
   b. Spry
   c. Spyglass
3. Applications Programming Interface (API)-level Toolkits -- Terisa
4. Developers Toolkits from RSA directly (see above)

C. Export -- The basic products from RSA's toolkit are not exportable (see "Export" item under other vendor listings for a more thorough list). There are exceptions:

1. In 1992, NSA approved the export of a limited version of RSA's product RC4

2. RSA and MIT have jointly developed a PGP-based version that gets around export problems and was released internationally. It is for personal use only.
3. RSA's CIS is exportable. The Japanese agent is Bug in Sapporo. Contact Kuskoor Bharath Ram at 81.11.807.6666

D. Users

1. National Semiconductor -- Developing credit-card-sized devices of microchips to encrypt data. These tokens verify purchases. Security is based on RSA.
2. Bankers Trust -- Bankers Trust Authentication System (BTAS) uses public key to develop its own digital signature system
3. Novell (Netware 4.0)
4. Sun Microsystems
5. Unisys Corp.
6. Apple Computer (Open Collaboration Environment OS)
7. Lotus Development (Notes)
8. Windows
9. NASDAQ uses RSA technology for a single log-on (contact Paul Fingerman, Director of Systems Architecture, Rockville, MD)
10. Adobe will embed RSA encryption and authentication into Acrobat 2.0 document distribution software (Telephone 415.962.2111)
11. Premenos Corporation (Concord, CA) using public key and digital signature to secure translator for EDI data (code named Templar) (Telephone 510.602.2000)
12. I-Link (Internet server provider), Round Rock, TX will use RSA encryption and authentication technology in browsers (Telephone 512.388.2393)
13. General Magic, Mountain View, CA (415.965.0400) develops Telescript technology for on-line retailing. Magic Cap, a more flexible EDI, and Telescript agents use RSA-licensed technology for encryption. In turn, AT&T has developed the PersonaLink network using telescript agents.

E. Contacts

1. Address: 100 Marine Parkway, Redwood City, CA 94065
2. Telephone

a. 415.595.8782 (Voice)

b. 415.595.1873 (Fax)

3. Contacts

a. Linda De Los Reyes, Sales, 415.688.4347

b. Web Augustine, Director of Marketing and Sales

II. Secure-Hypertext Transport Protocol (SHTTP)

A. Introduction

1. SHTTP is an extension of HTTP, providing independent security devices for transaction confidentiality, authentication, integrity, and non-repudibility of origin. HTTP is the transport protocol (See Attachment 2) for hypertext markup language (HTML) document formats which generally include universal resource names (URLs) that handle the links between documents.

2. A number of vendors have developed offerings for this technology. These vendors and their products are reviewed below.

B. Enterprise Integration Technology (EIT)

1. EIT is developing a toolkit based on RSA encryption software. EIT intends to provide a flexible SHTTP protocol that supports: key management methods, trust models, cryptographic algorithms, and encapsulated formats. Cryptographic message formats include PKCS-7, PEM, and PGM. Key components of their toolkit include:

a. Multiple operational modes -signature, authentication, encryption, or any combination

b. Signature - appropriate certificate attached to the message or handled independently

c. Encryption by two key transfer mechanisms:

i. One public key, in-band key exchange (symmetric key cryptosystem parameter is passed encrypted under the receiver's key)

ii. The other with externally pre-arranged session keys and key identification specified on a header

d. Message Integrity and Sender Authentication -- By computing the Message Authentication Code (MAC) computed as a keyed hashed over the document using a shared secret. (The secret can potentially be arranged manually or by Kerberos.)

e. Flexibility -- The protocol offers key management mechanism flexibility as well as security policy and cryptographic algorithms by supporting option negotiations between parties. For example, parties could agree to RSA vs DSA for signing, DES vs RC2 for encrypting, and even credit-card specific certification.

2. Marketing

a. Plans -- EIT plans to support a variety of implementation options to encourage widespread adoption. EIT is also actively creating turnkey applications (see CommerceNet below) that are deployed on top of EIT's SHTTP.

3. Export - EIT's toolkit is not exportable.

4. Users

a. The main direct user of EIT's technology is CommerceNet. CommerceNet is a non-profit, operating commercial network created and supported by a number of for-profit companies and partially underwritten by the U.S. Government. It intends to be a virtual hub to facilitate communications among companies, customers, suppliers, and developers and includes 128 Kbps ISDN lines for bandwidth to share multimedia. CommerceNet's approach, an on-line order form encrypted in such a way that only the merchant can decode it to find the buyer's unique digital signature, uses public-key technology. This software capability is usually packaged with the application. It does not have an environment for secure on-line financial transactions, although there are on-going discussions with CyberCash.

i. One issue, of course is to ensure that the person requesting the transaction (e.g., placing an order) is really that person.

ii. Some of the 80+ participants, and contacts when known, are:

- Bank of America -- Robert Winn 415.622.3530
- Citicorp -- 212 559 1000
- Lockheed
- National Semiconductor
- Pacific Bell
- Dun & Bradstreet
- Hewlett-Packard -- Sandy Wilson, EDI Business Manager, 415.857.1501

iii. CommerceNet may be reached at 415.617.8790

b. Terisa Systems is a joint venture of RSA and EIT. The Palo Alto, CA company "manages" CommerceNet. (Other founding developers include Mecklermedia Corp (Westport, CT), BARRNet, and Stanford University.)

5. Contacts

a. Telephone -- 415.617.8000

b. Contacts - Jay Marty Tenenbaum, CEO (Principal architect of SHTTP, the leading public-key encryption standard on WWW)

C. SPRY, Inc.

1. SPRY is currently beta-testing SafetyWEB, a SHTTP server. It is based on the non-proprietary RSA security scheme SHTTP licensed through TERISA. It includes functions for encryption, client and server authentication, and digital signatures (See Attachment 3). Specific features include:

a. It is based on the CERN's Web architecture.

b. Public key encryption provides for secure transfer of data over an unsecured network.

c. Both client and server authentication as well as basic authentication, allowing individuals without public keys the ability to authenticate with the use of a user name and password.

d. Access control lists that help administrators manage password verification.

e. Document caching and proxy servers supported for higher performance and Web server security.

2. Marketing

a. Plans - SPRY is actively marketing SafetyWEB through the Internet (See Attachment X) and in print media. A prototype of SafetyWEB is available as "public domain with copyright." Demonstrations and support are available for developers.

b. Pricing - No pricing has been established

3. Export - This product is not exportable. However, a similar version of the server, based on 40-bit keys, is also being beta tested and will be released in the second quarter of 1995.

4. Users - A key beta tester is Dun & Bradstreet Information Services (http://www.dbisna.com). D&B is offering free information on the Internet that includes business how-tos (e.g., international business, strategic planning, target marketing, credit management, supplier relationships, and job-search opportunities) and economic and trend information (e.g., economic and market segment growth, slow payment and business failures, risk in supplier portfolios, and job growth potential).

5. Contacts

   a. Address: 316 Occidental Avenue South, Seattle, WA 98104

   b. Telecommunications

      i. 800.SPRY.NET (800.777.9638)

      ii. 206.447.0300

      iii. 206.447.9008 (Fax)

      iv. Internet: info@spry.com

   c. Key Contacts

      i. Kevin Britt, Director of Marketing

      ii. Mark Goodman (mgoodman@spry.com)

D. Spyglass, Inc.

1. Spyglass licenses Mosaic from the University of Illinois and uses that platform for its own product, Enhanced Mosaic 1.0. Using their browser technology that intend to create tools for SHTTP. Enhanced Mosaic allows multiple encryption algorithms for SHTTP and authentication, but mostly the algorithms are from RSA. The product is available for Macintosh and Unix-based machines.

2. Marketing

a. Plans - Spyglass is actively marketing its product and trying to leverage earlier successes with the Air Mosaic browser and "Internet-in-a-box" tools for accessing Internet.

b. Pricing - The underlying product is licensed from the University of Illinois and so, by agreement, is sold on a per copy basis with a 10,000 copy minimum.

3. Export

a. Spyglass has two versions of this SHTTP: an enhanced authentication version that is not exportable and a version based on RSA's MD5 that is exportable without royalty. This version uses a 40-bit key and takes approximately 24 hours to break. (A third version using a simple template takes just one hour to break and is not further discussed here.)

b. NEC is a licensee in Japan. In addition, NTT Software Labs has a deal with Spyglass to localize Mosaic and offer it to other NTT divisions. The key contact for this effort is Masaki Itoh, Sr. Research Engineer. Spyglass is also interested in other technology relationships.

4. Users

a. AT&T has over 10,000 users of Enhanced Mosaic for Internet access.

b. A number of companies are using Spyglass methodologies as integral components for their products. In the financial arena these include:

i. First Virtual - This company offers an electronic wallet on WWW. After an out of band (off line) exchange of credit numbers, First Virtual acts as a clearing house, encrypting the passwords between transaction parties.

ii. NetBill, another WWW implementation of the methodology

iii. CyberCash -- Provides systems transactions servers to handle operations between vendors and customers on Internet. Their funds transfer uses encrypted electronic invoices and credit form based on RSA technology. They also are attempting to use tokens to symbolize cash. One credit authorization system in development is for Wells Fargo. Contact Steve Crocker (was with Trusted Information) at 703.620.4200 or 703.620.1222

5. Contacts

a. Address: 1230 E. Diehl Road, Suite 304, Naperville, IL 60563

b. Telecommunications

i. 800.647.8901 (V)

ii. 217 355 1665 (V)

iii. 708.505.1010 (V)

iv. 708.505.4944 (Fax)

v. e-mail: info@spyglass.com

vi. WWW: //http:www.spyglass.com

c. Key Contacts

i. Andy Parker, Business Development, 708.505.1010, Extension 505

ii. Tom Banahan (510 855 3240 or tbanahan@spry.com)

iii. Bob Rybicki or Mike Tyrell, Marketing

III. Secure Socket Layer

A. Introduction

1. Secure sockets layer (SSL) is an open security protocol suitable for use on the Internet and other TCP/IP networks in a broad range of contexts. It can be used with application-level protocols such as HTTP, FTP, Gopher, Telnet, NNTP, and many others. Most implementations support both servers and clients, although the current version doesn't support client authentication. It is based on RSAREF and is not exportable in this format. SSL and SHTTP are parallel security proposals.

B. Netscape (aka Mosaic Communications) is the leading vendor of this approach.

1. Product
   a. Netscape offers two product lines: Netscape Navigator (Version 1.0) browser/toolkit and the Netsite line of server software. Both are built on existing Internet standards such as TCP/IP communications protocol, HTTP server protocol, and HTML document format
      i. Navigator
         - Navigator supports both Netscape's Secure Socket Layer (SSL) security protocol as well as SHTTP in this browser/toolkit. Netscape is also considering adding full SHTTP support to the SSL implementation which would result in a general-purpose, dual-protocol security toolkit. Security technology is based on RSA technology. SSL include client-based encryption and server-based authentication. SSL was recently submitted to W3, the new security consortium (including MIT) for consideration as the standard.
         - Navigator is also backward compatible so it can communicate with HTP-based servers, FTP, Gopher, and NNTP-based Usenet. It is also compatible with HTTP-clients including Lynx, Cello, and Mosaic.
         - It displays multimedia in a variety of formats including GIF, JPEG, and MPEG.
      ii. Netsite Servers -- Neither the commerce server nor the communications server has security features; no further discussion is provided.
2. Market
   a. Plans -- Netscape plans to use Navigator to open the marketplace:
      i. The product is being giving away to non-profits
      ii. Netscape is trying to set the SSL as a standard through official bodies
      iii. Netscape is sharing security as "Request For Comments" and making it available on Internet
      iv. All client developments (protocols, interfaces, and specifications) will be open and publicly available

v. Netscape plans to support other protocols as well, making SSL robust

b. Pricing

i. Netscape is $39 for single user

ii. SSL and SHTTP toolkit is available free for non-commercial use.

iii. Commerce Server ($25k) includes RSA-based encryption and authentication

3. Export -- SSL is based on RSA's 80-bit encryption algorithm and is not exportable.

4. Users

a. MasterCard International -- Netscape working on system for them

b. Bank Of America and First Data are using Netscape -- Netscape helped create software to access First Data's on line credit card transaction service. This provides vendors and customers with the means to exchange credit card information on the Internet

c. Netscape protocols are also included in the following operating systems:

i. Windows

ii. System 7

iii. X-Windows

5. Contacts

a. Address: Mountain View, CA

b. Telecommunications

i. 415.254.1900 or 415.528.2555 (Voice)

ii. info@netscape.com

iii. http://home.mcom.com/

iv. http://mcom.com/info/security-doc.html

v. http://mcom.com.info/ssl.html

c. Contacts

i. Rosanne Siino (Public Relations) 415.254.2619

. info@netscape.com

ii. James H. Clark, Chief Executive Officer

IV. Privacy Enhanced Mail

A. Internet Privacy-Enhanced Mail (PEM) is a proposed, but not yet adopted standard of the Internet Activities Board. It provides secure electronic mail over the Internet. It is designed to work with current Internet electronic mail formats. PEM includes encryption, authentication, and key management and allows users of both public-key and secret-key cryptosystems. Multiple cryptographic tools are supported: for each mail message the specific encryption algorithm, digital signature algorithm, hash function, and so on are specified in the header. PEM explicitly supports only a few cryptographic algorithms: DES in CBC mode is the only message encryption algorithm, RSA and DES are both supported for key management, and PM supports the use of CCITT X.509-standard certificate structures.

B. Vendors

1. RIPEM, developed by Mark Riordan, enables secure Internet mail providing both encryption and digital signatures, but not certificates. It is not currently fully PEM-compatible, but future versions with certificates and full PEM-compliance are planned. It uses RSA and DES routines. The RSA cryptographic routines are from a toolkit, RSAREF, that cannot be used commercially or sent outside the U.S. and Canada.
2. RIPEM is available via FTP at ripem.msu.edu. RSAREF is available to U.S. citizens by e-mail to rsaref@rsa.com or by FTP to rsa.com.

C. Trusted Information Systems (TIS)

1. TIS provides privacy-enhanced mail, a product than can't be exported.
2. TIS also provides an alternative to the Clipper chip. This Unix-based signature system, Commercial Key Escrow, allows encryption with no government involvement. The "escrow" feature, by using a public-key to attach a Law Enforcement Access Field (LEAF), has the trap door the U.S. Government seeks, but has more flexibility and a lower price.
3. Contacts

a. Address: Glenwood, MD

b. Telecommunications

i. 301.854.6889

ii. netsec.tis.com or tis/pem (for FTP version)

c. Contacts

i. James P. Litchko, Director of Marketing

ii. Stephen Walker, President

V. Others

A. Public-Key Cryptographic Standards (PKCS) is a set of RSA-supplied standards issued in cooperation with a computer industry consortium including Apple, Microsoft, DEC, Lotus, Sun, and MIT. It is a method of implementing OIS standards and is compatible with PEM. It intends beyond PEM to handle binary data (PEM only handles ASCII) and is compatible with the CCITT X.509 standard. PKCS includes both algorithm-specific and algorithm-independent implementation standards and supports RSA, DES, and Diffie-Hellman key exchange. It also defines algorithm-independent syntax for digital signatures, digital envelopes, and certificates. Documents detailing the standards are available via e-mail to pkcs@rsa.com or by anonymous FTP to rsa.com.

B. Kerberos

1. Kerberos is a secret-key network authentication system developed at MIT. It uses DES encryption and authentication but, unlike public-key authentication, does not produce digital signatures. It was designed to authenticate requests for network resources rather than to authenticate documents. It provides real-time authentication in a distributed environment, but does not provide for future third-party verification of documents.

2. In a Kerberos system, there is a designated site on the network, called the Kerberos server, which performs key management and administrative functions. The server maintains a database containing the secret keys of all users, generates session keys whenever two users wish to communicate securely, and authenticates the identity of network resource requesters. Kerberos requires trust in a third-party, the Kerberos server.

C. Message Digest X (MD2, MD4, MD5)

1. These are hash functions developed by Ron Rivest of RSA. (A hash function is a computation that creates a message digest that represents concisely the longer message or document from which it was computed; a "digital fingerprint" for authentication.) These MD products produce 128-bit digests, but differ in speed and design. MD2 is used with PEM, but MD4 and MD5 are publicly available for unrestricted use.

D. Certificates

1. Certificates are digital documents for verification of the claim that a given public key belongs to a given individual. Certificates help prevent someone from using a false key to impersonate someone else. They usually contain a public key, the name, expiration date of the key, name of the Certifying Authority, serial number of the certificate, and, most importantly, the digital signature of the certificate issuer, etc.
2. The most secure use is to enclose one or more certificates with every signed message. The message receiver verifies the certificate using the Certifying Authority's public key. Two or more certificates in a message creates a hierarchical chain wherein one certificates attests to the authenticity of the previous certificate.
3. The Certifying Authority is a trusted central administration; an employer, a university, a bank. To prevent forged certificates, the Authority's public key must be trustworthy.
4. Vendors
   a. Apple Computer's Open Collaborative Environment is a certificate-issuing protocol
   b. Bolt, Beranek, and Newman (BBN) sells a certificate signing unit (CSU)
   c. RSA Data Security sells a full-fledged certificate issuing system built around the BBN CSU.

E. Digital Time-Stamping Service (DTS)

1. While not a method for secure payments, DTS is a means to prove than an electronic document existed at the time stated on its time-stamp. Generally, the message digest is sent to the DST which, in turn, sends back the digest, date/time it was received by the DTS, and the signature of the DTS. Later, a verifier computes the message digest and matches the digest to the time stamp.
2. Bellcore has Digital Time-Stamp software for practical and foolproof electronic document security. Contact Michael Ressler, Secure Communications and Services Group.

VI. What methods are dominant now? In the future?

A. For electronic commerce to flourish on an open data network such as Internet, solutions must be developed so that any end node attached to the network can mitigate its risk to an acceptable level. These risks include both reliability and vulnerability. While the two issues are interrelated, the focus of this discussion is on the latter and, specifically, controlling the threat of fraud in electronic commerce. This threat is located at two points, the data and systems at each node that intend to have both publicly available and inaccessable components, and the integrity and authenticity of the data that is actually transported over the network and represents the transactions of commerce. Again, these issues are related, but the discussion centers on current and future methods of integrity and authenticity.

B. Reducing the level of risk requires some investment of time or money on the part of the vendor and some additional difficulties on the part of users (e.g. slower speed, more complexity). A security solution that is "foolproof" may be too expensive to develop and too complex to use. A solution that is easy to use, but not safe, will not be used. The optimum solution seems to be a point where the risks are at tolerable levels for both parties (vendor and user) while the "costs" of offering and using these services are as low as possible. There are a number of possible solutions scattered around this optimum point. These are discussed below according to whether they tend to favor security or ease of use.

1. Security, and then Ease of Use

a. Protection of information "in the network" is currently managed by single approaches: message cryptography, user authentication, or user certification. Selection generally depends on cost; overhead; convenience; level of security needed, given the value of the information, and length of time it needs to be secure. Typically the decision is based on balancing these criteria with the work factor required for an attacker to gain access to the secured information. The work factor can be increased by, for example, varying the length of the key, using various methods to generate the key, or the complexity of the algorithm processing. The tradeoff is the time that these take vs. their security value. In fact, the DES standard is that security be provided by the algorithm, not be based on its secrecy. The DES and RSA algorithms are widely known, but the domain of possible solutions is so large that factoring searches are very expensive and time-consuming.

b. Since the processing complexity is highly dependent on the speed of the computers used, it is likely that methods will grow more complex as processing costs drop. However, since processing cost declines help both in the creating and attacking, it seems likely that cost reductions will not play a significant part in the dominant methods of the future.

c. The trend seems to be the deployment of multiple methods: message encryption, authentication, certification. These multiple hurdles will act to "discourage" all but the most zealous hackers or terrorists. And, with integrated systems in development, it may be possible for multiple methods to be applied to a given transaction at a cost that is a fraction of all three. Under the best approaches, these three methods in then same transaction would each require a considerable effort on the part of the attacker.

d. A likely scenario might be to encrypt the plaintext to cybertext by public/private key pair: recipient's public key for privacy and sender's private key for digital signature, hash the digital signature, and then use a single key to transform everything into cybercode.

e. A second trend gaining popularity is to create dynamic keys with time-to-live features. Each key has a defined life span (e.g., a few hours, a day) during which it is valid. At the end of that time, the key "dies" and is no longer useful. Code management schemes based on one-time or time-of-day schemes are currently in use. The philosophy behind this strategy is that as along as the time-to-live is shorter than the time it takes to break the code, it would be useless to try to decypher since the transactions will have been completed. This notion is attractive since it doesn't add to the complexity of the process, but does heighten discouragement for would-be villains.

f. A third approach is to employ a second security system, generally embedded in hardware, that holds an authentication key. SecureNet Key, developed by Digital Pathways, Mountain View, CA) is one type of "challenge response" system that uses an authentication calculator using DES. National Semiconductor offers the PCMIA-based PersonaCard. SecureID (Security Dynamics, Cambridge, MA, 617 547 7820) couples encryption and time-based codes in an access control card that generates a random code every 60 seconds, requiring user must present the latest code to gain entry to subsequent transactions. In systems where similar features are implemented on a smart card and a server, the two are always synchronized. This adds additional safety to single log-on systems that can span an entire network for unauthorized users.

2. Ease of use, then Security

a. One philosophy in this camp is "security through obscurity;" there are so many messages pouring through the Internet each day that it would be virtually impossible for a hacker to find the ones with financial information (e.g., credit card numbers). Carried to its extreme, this view is no (or minimum) security is needed. This, in turn will encourage more users, more transactions, and more obscurity. This is a radical position that is unlikely to be embraced by many vendors. Proponents say any key management will impede or discourage transactions (e.g., consumers will resist the impulse to purchase).

b. A better approach, some believe, is the equivalent of on-line credit cards good at participating merchants; that is, financial information is exchanged "out of band" (i.e., outside the network through, say, a ground courier). The transactions then involve ordering by calling the computer that has the credit number. That computer will, in turn, call you back to confirm and authenticate the order. Opponents think the technology should be used for all things and that such a solution simply reverts businesses to current practices.

c. A third approach is the electronic equivalent of cash. In this approach a consumer withdraws funds from a bank into a digital account on the consumer's personal computer. Purchases are made through vendors who accept this digital cash. Proponents say this is a simple answer for the mass market where the bulk of purchases will be inexpensive. While the small amounts of money that could be stolen from an individual node would tend to discourage hackers and limit losses, this scenario does not seem to fit the industrial model of money transfers where tens of millions of dollars could be involved. Also, this solution simply moves the focus of the problem to the wall separating the vendor's public and private systems. Will vendors' firewalls be able to sustain attacks?

C. Finally, regardless of the strategy, there are practical matters of business to contend with in implementing a security approach. Logistics, for example. Imagine the issues that could arise just in distributing an out-of-band key or other encryption device. Some will be lost, stolen, misplaced, nonfunctional, etc. When keys are available, either in- or out-of-band, vendors and users will not only need to contend with most of the issues mentioned above (i.e., stolen, forgot how to use), but also all of the problems associated with an ever-increasing transient work force; people are hired, fired, move, etc. Given the many practical implementation issues, the approach and subsequent usage of a secured system may depend on something as simple as the trust that vendors and users have for each other.

APPENDICES

A. Glossary

1. Authentication -- process to establish the validity of a claimed identity
2. Browser -- generic name for software supporting the navigation among hyperlinked documents
3. Cypher block chaining (CBC) -- process of relating a plaintext block with the previous cybertext before encrypting it
4. Conseil Europeen pour la Recherche Nucleaire (CERN) --Swiss organization, now called European Laboratory for Particle Physics, which originally proposed HTTP
5. Certificate -- digital document verifying that a key belongs to a given individual
6. Certificate issuing system (SIS) -- creates digital certificates enclosed with messages
7. Digital encryption standard (DES) -- standard supported by the U.S. Government
8. Digital signature or digital fingerprint) -- a unique, encrypted component of a message used for authentication
9. Digital signature standard (DSS) -- U.S. Government-proposed standard specifying a digital signature authentication algorithm
10. Digital time-stamp (DTS) -- process of electronically verifying that a document existed at a certain time
11. Domain name system (DNS) -- method used to convert Internet names to their corresponding numbers
12. Encryption -- transformation of data into a secret code
13. File transfer protocol (FTP) -- common protocol used for sharing files on the Internet
14. Gopher -- software for navigating text-based documents linked to one another through URLs
15. Hashing -- a computational process that creates an encrypted digest of the message for later tamper evidence
16. Hypertext markup language (HTML) -- hypertext markup language for document formats
17. Hypertext transfer protocol (HTTP) -- transport format for HTML
18. Kerperos -- secret-key network authentication management system

19. Message authentication code -- a secret key hashed over a document
20. Mosaic -- a WWW multimedia browser created at the University of Illinois
21. National Security Agency (NSA) -- highly secretive agency of the U.S. Government responsible for listening to and decoding all foreign communications of interest to the security of the U.S.
22. Network Information Center (NIC) -- a "hub" on Internet
23. News network transfer protocol (aka hypertext news transport protocol, HNTP) -- format for accessing documents on Usenet
24. Ping -- a program that traces message routes
25. Pretty good privacy (PGP) -- exportable, low-end encryption algorithm created by Philip Zimmerman and distributed for free on Internet (ViaCrypt makes a commercial version)
26. Privacy-enhanced mail (PEM) -- proposed standard for secure mail over the Internet
27. Public-key cryptographic standard (PKCS) -- standards of public-key cryptography issued by RSA
28. Private (secret) key -- encryption key management system where keys are exchanged before the message encryption between individuals
29. Public key -- encryption key management system where messages are encoded by public keys available to anyone and decoded only by a private key available to the message recipient
30. Secure sockets layer (SSL) -- security protocol operating at the application/network interface with TCP/IP networks
31. Secure hypertext transfer protocol -- secure version of HTTP
32. Simple mail transfer protocol (SMPT) -- Internet-standard for transferring electronic mail messages
33. Serial line Internet protocol (SLIP) -- used to turn computers into Internet sites over telephone lines
34. Telnet -- program that provides computer interconnection on the Internet
35. Transmission control protocol/internet protocol -- message/file transfer protocol on Internet

36. Trusted network -- secure communication as established by a security policy

37. Universal resource locator (URL) -- format for links in a document to other documents or resources (multimedia, files, etc.)

38. World wide web (WWW) -- subset of Internet linked together by multimedia URLs in HTML documents under HTTP

APPENDICES

A. Attachments

1. RSA Data Security literature
2. Secure HyperText Transfer Protocol
3. SPRY, Inc. copies of WWW pages